Leviathan Wargame Report (Level 0 to Level 7)

Using Kali Linux Terminal

Level 0

- **Steps:**
  - Logged into Leviathan 0 via SSH.
  - Moved to /home/leviathan0.
  - Listed the files using ls.
  - Read the README file using cat for further guidance.
- **Tools Used:**
  - SSH
  - ls
  - cat
- **Logic Behind the Solution:**
  - Found initial clues in the README file to guide the next steps.

Level 1

- **Steps:**
  - SSH'd into Leviathan 1.
  - Navigated to /home/leviathan1.
  - Listed all files, including hidden ones, using ls -la.
  - Read files using cat to search for hidden clues or passwords.
- **Tools Used:**
  - ls -la
  - cat
- **Logic Behind the Solution:**
  - Focused on uncovering hidden files that might contain clues or passwords.

Level 2

- **Steps:**
  - Logged into Leviathan 2.
  - Went to /home/leviathan2.
  - Listed available files using ls.
  - Checked the README file.
  - Searched for hidden or suspicious files.
- **Tools Used:**
  - ls
  - ls -la
  - cat
- **Logic Behind the Solution:**
  - Inspected hidden files for further clues or hints.

Level 3

- **Steps:**
  - SSH'd into Leviathan 3.
  - Moved to /home/leviathan3.
  - Listed all files using ls -la.
  - Read files using cat to explore content in detail.
- **Tools Used:**
  - ls -la
  - cat
- **Logic Behind the Solution:**
  - Carefully examined all files, both visible and hidden, to find clues.

Level 4

- **Steps:**
  - Logged into Leviathan 4.
  - Navigated to /home/leviathan4.
  - Listed and read files, including the README.
  - Used grep and strings to find hidden content.
- **Tools Used:**
  - ls -la
  - cat
  - grep
  - strings
- **Logic Behind the Solution:**
  - Used strings and grep to search for hidden messages or clues inside files.

Level 5

- **Steps:**
  - Logged into Leviathan 5.
  - Explored the /home/leviathan5 directory.
  - Listed all available files including hidden ones using ls -la.
  - Analyzed files for hidden data or clues.
- **Tools Used:**
  - ls
  - ls -la
  - cat
  - strings
  - grep
- **Logic Behind the Solution:**
  - Focused on finding hidden data or binary clues and decoding them.

Level 6

- **Steps:**
  - SSH'd into Leviathan 6.
  - Navigated to /home/leviathan6.
  - Listed files using ls -la.

    - Used content analysis (cat, grep, strings) to look for clues.
- **Tools Used:**
    - ls -la
    - cat
    - grep
    - strings
- **Logic Behind the Solution:**
    - Searched through hidden files for encoded or encrypted data.

Level 7

- **Steps:**
    - Logged into Leviathan 7.
    - Listed files in /home/leviathan7 using ls and ls -la.
    - Focused on extracting hidden or encoded messages.
- **Tools Used:**
    - ls
    - ls -la
    - cat
    - strings
- **Logic Behind the Solution:**
    - Extracted and decoded hidden messages that led to the solution.